

What is claimed is:

1. A random number generator comprising:

5 a plurality of pseudo-random number generating unit capable
of respectively outputting random numbers of a fixed pseudo-random
number sequence;

output random number generating unit capable of generating an
output random number based on output of the plurality of pseudo-random
number generating unit;

10 physical random number generating unit for generating a
physical random number; and

switching unit for, in generation of an output random number
in the output random number generating unit, switching whether or not
a pseudo-random number generated by at least one of the pseudo-random
15 number generating unit is used based on a physical random number
generated by the physical random number generating unit.

2. The random number generator of claim 1, wherein the switching unit
switches whether or not a clock signal is input to at least one of
20 the pseudo-random number generating unit based on the physical random
number.

3. The random number generator of claim 1, wherein a physical random
number generated by the physical random number generating unit is input
25 as a clock signal of at least one of the pseudo-random number generating
unit.

4. The random number generator of claim 1, wherein the switching unit switches whether or not a pseudo-random number generated by at least one of the pseudo-random number generating unit is input to the output random number generating unit based on the physical random number.

5

5. The random number generator of claim 1, wherein the output random number generating unit is an exclusive OR gate.